AF/2700
#11
2-11-03
1 of 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

JAMES P. HUGHES

Group Art Unit: 2132

Examiner: J. T. Darrow

Serial No.: 09/260,796

Filed: March 1, 1999

For: Method and System for Secure Information Handling

Attorney Docket No.: 98-019-NSC (STK98019PUS)

APPEAL BRIEF

Box AF
Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231

Sir:

This is an appeal brief from the final rejection of claims 1-5, 7, 10, 11, 13 and 15-17 in an Office Action dated August 26, 2002. This application was filed on March 1, 1999.

I. REAL PARTY IN INTEREST

The real party in interest is Storage Technology Corporation, a corporation organized and existing under the laws of the state of Delaware, and having a place of business at 2270 South 88th Street MS-4309, Louisville, Colorado 80028-4309, as set forth in the assignment recorded in the U.S. Patent and Trademark Office on March 1, 1999 at Reel

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Box AF, Commissioner for Patents, United States Patent and Trademark Office, Washington, D.C. 20231 on:

January 31, 2003 — Date of Deposit
Mark D. Chuey, Ph.D. — Name of Person Signing
Signature

9801/Frame 0575.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences related to the present appeal.

III. STATUS OF CLAIMS

Claims 1-17 are pending in this application. Claims 1-5, 7, 9- 11, 13 and 15-17 have been rejected and are the subject of this appeal. Claims 6, 8, 12 and 14 were objected to as being dependent upon a rejected base claim but otherwise as containing allowable subject matter.

IV. STATUS OF AMENDMENTS

No amendment was filed after final rejection.

V. SUMMARY OF THE INVENTION

The present invention provides for the secure handling of information encrypted to a data set. The data set is stored on at least one storage device, typically an untrusted storage device. At some point, the information is requested by a consumer client. In order to obtain the information, a value required to decrypt the information is decrypted by correctly solving an access formula describing a function of one or more groups. Each group includes a list of at least one client. The requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula.

With regards to Figures 1, 3 and 6, the invention may be further described as follows. Each client 42, 44 is connected to at least one untrusted storage device 62 using a network 20. The network further has associated therewith a key manager 66 for issuing private key 88 and public key 86 matched pairs for use with an asymmetric encryption and

decryption scheme. This scheme allows a file encrypted with a public key 86 to be decrypted only with a matched private key 88.

Each group 82 includes a list 90 of at least one consumer client 44. A public key 86 and a matched private key 88 is acquired for each group 82.

An information set is encrypted to produce a data set 98 based on a randomly generated number 100. An access formula 102 is determined expressing a logical combination of at least one group 82 for which access to the encrypted information set 96 will be granted. Solution of the access formula 102 by at least one solution group 82 indicates that a consumer client 44 belonging to the solution group 82 may access the encrypted information set 96.

The randomly generated number 100 is asymmetrically encrypted using the access formula 102 and the public key 86 for each group 82 granted access to the information set 96. A randomly generated number 100 so encrypted is added to the data set 98. The data set 98 is stored on at least one untrusted storage device 62.

When a request is received from the consumer client 44, a determination is made as to whether or not the consumer client 44 belongs to at least one solution group 82 which solves the access formula 102. If not, access is denied. If so, the randomly generated number 100 is decrypted using the private key 88 for the at least one determined solution group 82.

The access formula is discussed with regards to Figure 4 on page 15, lines 11-17, as follows:

> Access formula 102, also known as an access control list or ACL, expresses a logical combination of groups 82 and clients 22 for which access to encrypted information 96 will be granted. Solution of access formula 102 indicates that consumer client 44 is either specified as client 22 directly granted to access encrypted information 96 in access formula 102 or is a member of group 82 granted access to encrypted information 96 by access formula 102.

The need for such an access formula is disclosed on page 10, lines 10-25, as follows:

> Another design challenge is the ability to permit access to information based on combinations of groups of clients 22. A group may be defined as those clients 22 which share a common mandate. For example, possible groups may be all members of

the financial department, members of the Board of Directors, software engineers assigned to project X, and the like. It is desirable to permit access to information based on combinations of groups such as, for example, clients which are either members of the Board of Directors or are members of both project X and are senior software engineers. Another useful form of description is to permit access to any client which is a member of M-of-N groups. For example, a client 22 may be granted access if it is a member of any two-of-three groups, Group 1, Group 2, and Group 3. It will be recognized that one of ordinary skill in the art can express access to information as a boolean combination of groups. A group asserts true in the boolean combination when consumer client 44 which is a member of the group requests access to the information set protected by the access formula. Consumer client 44 may then be granted access to the information if the access formula resultant is true.

VI. ISSUES

The following art, cited in the Examiner's rejections of claims 1-5, 7, 9- 11, 13 and 15-17, is referenced in this brief: U.S. Patent No. 5,787,175 to Carter (henceforth referred to as Carter) and U.S. Patent No. 3,798,360 to Feistel (henceforth referred to as Feistel). The Examiner's rejections suggest that the following issues are presented for appeal:

1. Whether or not claims 1, 2, 9-11, 13 and 15-17 are properly rejected under 35 U.S.C. § 102(e) as being anticipated by Carter.

2. Whether or not claims 3-5, 7 and 10 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Carter in view of Feistel.

VII. GROUPING OF CLAIMS

The following claims are grouped to stand or fall together:

Group A: Claims 1 and 2.

Group B: Claims 9, 10, 13, 15-17.

Group C: Claim 11.

Group D: Claims 3-5.

Group E: Claim 7.

VIII. ARGUMENT

In a final Office Action dated February 8, 2002, the Examiner rejected claims 1-5, 7, 9- 11, 13 and 15-17 in the above-captioned patent application. Appellants disagree with these rejections based on the following arguments.

1. Whether or not claims 1, 2, 9-11, 13 and 15-17 are properly rejected under 35 U.S.C. § 102(e) as being anticipated by Carter

The Examiner rejected claims 1, 2, 9, 11, 13 and 15-17 under 35 U.S.C. § 102(e) as being unpatentable over Carter. As the following detailed arguments indicate, this is not the case.

A. Whether claim 1 is unpatentable under 35 U.S.C. § 102(e) over Carter

Claim 1 provides a method for the secure handling of information encrypted to a data set such that the information may be requested by a requesting consumer client. The data set is stored on at least one storage device. The method includes decrypting a value required to decrypt the information. The value is decrypted by correctly solving *an access formula describing a function of groups*. Each group includes a list of at least one client. The requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula. Carter neither teaches nor suggests Appellant's access formula.

The Examiner's support that Carter discloses Applicant's access formula is provided on page 2 (and again on page 5) as follows:

> Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

There are several problems with the Examiner's argument.

i. Carter does not teach Appellant's access formula describing a function of groups

Claim 1 provides for an access formula describing a function of groups. Assuming, *arguendo*, that Carter inherently teaches comparing a password with some stored value, such a comparison does not teach or suggest an access formula describing *a function of groups*. In fact, such a simple comparison teaches away from the use of any mathematical or logical combination or function of groups.

ii. Carter does not teach Appellant's formula for gaining access

Carter does not teach a *formula* for gaining access. The passages and figures cited by the Examiner do not mention, in any manner, a formula of any kind. The text at column 16, lines 16-29, is reproduced as follows:

> After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. As with other portions of the collaborative access controller 44, the portion which performs the obtaining step 152 may be embodied within the application 52 or may be a separate module which is invoked by the application 52 or by the user. The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password. In alternative

> embodiments, the user identifier identifies the current user and is obtained by querying the operating system 46 or the object database system 62; only the password is obtained interactively from the user.

This passage has nothing whatsoever to do with an access formula. At best, this is a routine collection of user ID and password. The Examiner also cites Figure 4, reference 90, which is described as follows at column 12, lines 9-14:

> FIG. 4 illustrates a work group document 90, also known as "collaborative document 90," which is configured according to the present invention. The work group document 90 includes a prefix portion 92 and a data portion 94. The prefix portion 92 and the data portion 94 are each capable of being stored in at least one file in the computer system 10 (FIG. 1).

Again, not even a hint of a formula of any kind. Finally, the Examiner cites Figure 9, step 152, which bears the text "OBTAIN USER IDENTIFIER AND PASSWORD FROM USER WHO SEEKS ACCESS." Yet again, not even a hint of a formula of any kind.

The Examiner states that Carter's alleged password matching "is within the scope of an access formula as described by the applicant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 24)." (Page 2.) Items 22 and 24 in Figure 1 are described as follows on page 9, lines 12-18:

> Referring now to Figure 1, a diagram of a computer network that may use the present invention is shown. Computer network 20 includes a plurality of clients, shown generally by 22. Clients 22 may include users working on a computer which is part of computer network 20, application programs running on computers which are part of computer network 20 accessing information on behalf of a user, and automated systems which are part of computer network 20. Client systems 22 are interconnected through hubs 24 and routers 26 to form computer network 20.

How this supports the Examiner's definition of an access formula is not discernable. The passage cited by the Examiner from page 10 is as follows:

> Another design challenge is the ability to permit access to information based on combinations of groups of clients 22. A group may be defined as those clients 22 which share a common

> mandate. For example, possible groups may be all members of the financial department, members of the Board of Directors, software engineers assigned to project X, and the like. It is desirable to permit access to information based on combinations of groups such as, for example, clients which are either members of the Board of Directors or are members of both project X and are senior software engineers. Another useful form of description is to permit access to any client which is a member of M-of-N groups. For example, a client 22 may be granted access if it is a member of any two-of-three groups, Group 1, Group 2, and Group 3. It will be recognized that one of ordinary skill in the art can express access to information as a boolean combination of groups. A group asserts true in the boolean combination when consumer client 44 which is a member of the group requests access to the information set protected by the access formula. Consumer client 44 may then be granted access to the information if the access formula resultant is true.

As this passage indicates, access formulas may be boolean combinations of groups. Access is granted only if the logical expression is true. This is not a simple comparison of a supplied password with a stored value, as asserted by the Examiner. Thus, the Examiner has failed to indicate any teaching in Carter for an access *formula*.

iii. The Examiner abused his discretion in claiming an inherent teaching

The Examiner abused his discretion by not finding a teaching of Applicants' access formula.

> "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (citations and U.S.P.Q. cite omitted).
>
> M.P.E.P. § 2112.

Thus, an "access formula," by whatever definition is used, is inherent in Carter only if this is the only possible method by which a password may be verified. It is not. For example, the password may be an encoded version of the user identifier. In this case, the computer system decodes the password and compares it with the identifier. No comparison with a stored value is necessary. Since password verification methods exist which do not, as the Examiner claims, "have to be compared with a stored value in order to determine granting user access," an "access formula," even as broadly defined by the Examiner, is not inherent in Carter.

Claim 1 is patentable over Carter. Claim 2 depends from claim 1 and is therefore also patentable.

B. Whether claim 9 is unpatentable under 35 U.S.C. § 102(e) over Carter

Independent claim 9 provides a system for the secure handling of information stored on at least one untrusted storage device connected to a network. A key manager, connected to the network, generates private key and public key matched pairs for use with an asymmetric encryption and decryption scheme. This scheme allows a file encrypted with a public key to be decrypted only with a matched private key. At least one group server is connected to the network. Each group server maintains at least one group with a list of client members allowed access to information produced by any client member of the group and obtains a private key and matched public key for each group. At least one producer client is connected to the network. Each producer client encrypts an information set to produce a data set, the encryption based on an encryption value; determines an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a client belonging to the at least one solution group may access the encrypted information set; asymmetrically encrypts the encryption value using the determined access formula and the public key for each of the at least one group for which access to the information set may be granted; adds the encrypted encryption value and the access formula to the data set; and stores

the data set on at least one untrusted storage device. Carter does not teach claim 9 for the following reasons:

i. Carter does not teach Appellant's group server obtaining keys for each group

Claim 9 provides, *inter alia*, a group server obtaining a private key and matched public key for each group. It appears that the Examiner has provided no teaching or suggestion for such acquisition[1]. In fact, Carter teaches obtaining a public key and a private key only for each *group member*, not each group. For example, column 13, line 63-column 14, line 5, is as follows (emphasis added):

> The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the *public key of the member in question.*, which was obtained during the step 116. Note that the underlying document key is the same for each *member of the collaborative group*, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key.

Public key 78 and private key 80 are obtained for each group *member*, as is described at column 13, lines 29-46, a portion of which is reproduced as follows:

> During a member-key-obtaining step 116, the collaborative access controller 44 obtains one public key 78 for each collaborative group member. . . .
> * * * *
> In another embodiment, the collaborative access controller 44 makes requests for public keys 78 directly to the object database system 62 without going through the authenticator 64. In alternative embodiments, the public key 78 is obtained from the operating system 46, the hardware token 32 (FIG. 1), or the

[1]Typically, an examiner makes a rejection by stating each claim element and then providing a teaching or suggestion for that element. This Examiner, however, chooses instead to use only the language of the cited art in stating his rejections. Hence, it is difficult to determine the Examiner's theory as to how the cited art matches up with each claim element.

> PCMCIA card 30 without accessing the database system 62. Similar steps are employed to obtain private keys 80 during other steps described hereafter.

Nowhere in Carter does a private key appear to be used with a group.

ii. Carter does not teach Appellant's formula for gaining access

Claim 9 provides, *inter alia*, for an access formula expressing logical combination of at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a client belonging to the at least one solution group may access the encrypted information set. Carter does not teach a *formula* for gaining access.

The Examiner's support that Carter discloses Applicant's access formula is provided on page 3 as follows:

> Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

This argument was refuted in subsections ii and iii of section A above.

Claim 9 is patentable over Carter. Claims 13, 15-17 depends from claim 9 and are therefore also patentable. Carter does not disclose a group server obtaining a private key and matched public key for each group. Thus, even if claim 1 is deemed unpatentable, claim 9 is still patentable.

C. Whether claim 11 is unpatentable under 35 U.S.C. § 102(e) over Carter

Claim 11, which depends from claim 9, provides a system for the secure handling of information wherein *the access formula is a boolean combination of groups*. A

group asserts true in the boolean combination when a client member of the group requests access to the information set protected by the access formula. The client member is granted access if the access formula resultant is true.

Claim 11 provides for an access formula that is *a boolean function of groups*. The Examiner cannot find any such teaching in Carter, as stated on page 6 as follows:

> As per claim 11, Carter points out that the member is verified if the corresponding identifier is found . . . Carter does not explicitly disclose the feature of a boolean combination resultant of true [*sic*]. However, this feature is deemed to be inherent to the system of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The system of Carter would be inoperative if this logical consequence did not result. Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

Figure 4 illustrates document 90 which includes prefix 92 having member definitions 96. Figure 5 illustrates member definition 96 as having member identifier 98, encrypted document key 100 and encrypted message digest 102. Figure 9 is a flow diagram including step 152, "OBTAIN USER IDENTIFIER AND PASSWORD FROM USER WHO SEEKS ACCESS," and step 154, "ATTEMPT TO OBTAIN USER'S PRIVATE KEY." The passages cited by the Examiner are as follows:

> In the preferred embodiment, according to which any current member of a collaborative group has authority to change the membership of the group, the verifying step 140 includes searching the member definitions 96 in the prefix portion 92 of the work group document 90 for a member identifier 98 that corresponds to the user who is requesting the change in group membership. If a corresponding member identifier 98 is found, the user is authorized to make the request. Otherwise, the user is not a member of the collaborative group and thus is not authorized to request changes in the membership of that group.

Col. 15, ll. 47-51.

> After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. As with other portions of the collaborative access controller 44, the portion which performs the obtaining step 152 may be embodied within the application 52 or may be a separate module which is invoked by the application 52 or by the user. The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password. In alternative embodiments, the user identifier identifies the current user and is obtained by querying the operating system 46 or the object database system 62; only the password is obtained interactively from the user.

Col. 16, ll. 16-29.

> If the key-seeking step 154 succeeds, a member-seeking step 158 is performed. The step 158 searches the member definitions 96 of the collaborative document 90 in an attempt to locate a member identifier 98 that corresponds to the user identifier obtained during the step 152. The search is accomplished substantially as described above in connection with the steps 122, 140, 142. If the search fails, then the user identifier does not identify a member of the collaborative group and the limiting step 156 is performed.
> If the search succeeds, a key-decrypting step 160 is performed.

Col. 16, ll. 51-62.

While Carter may disclose finding and comparing a member identifier, this in no manner teaches or suggests an access formula based on a boolean combination of groups. Carter does not teach or suggest an access formula of any kind, let alone one based on a function of groups. Further, the Examiner is abusing his discretion by asserting that any such function is inherently disclosed. There are clearly any number of ways a user may be granted access. Thus, it is improper for the Examiner to imply that Appellant's access formula is disclosed simply because Carter is inoperative but for some form of access control.

Claim 11 is patentable over Carter. Carter does not disclose an access formula that is a boolean function of groups. Thus, even if claim 16 is deemed unpatentable, claim 11 is still patentable.

2. Whether or not claims 3-5, 7 and 10 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Carter in view of Feistel

The Examiner rejected claims 3-5, 7 and 10 under 35 U.S.C. § 103(a) as being unpatentable over Carter in view of Feistel. As the following detailed arguments indicate, no combination of Carter and Feistel teach or suggest Appellant's invention.

D. Whether claim 3 is unpatentable under 35 U.S.C. § 103(a) over Carter in view of Feistel

Claim 3 provides a method for the secure handling of information by at least one client using at least one untrusted storage device. Each client is connected to the at least one untrusted storage device using a network. Associated with the network is a key manager for issuing private key and public key matched pairs for use with an asymmetric encryption and decryption scheme. This scheme allows a file encrypted with a public key to be decrypted only with a matched private key. At least one group is created. Each group includes a list of at least one consumer client. A public key and a matched private key is acquired for each group. An information set is encrypted to produce a data set based on a randomly generated number. An access formula is expressing logical combination of the at least one group for which access to the information set will be granted is determined. Solution of the access formula by at least one solution group indicates that a consumer client belonging to at least one solution group may access the encrypted information set. The randomly generated number is asymmetrically encrypted using the determined access formula and the public key for each group granted access to the information set. The encrypted randomly generated number is added to the data set. The data set is stored on at least one untrusted storage device.

In rejecting claim 3, the Examiner indicated that Carter did not disclose the use of a random number as an encryption key. For this purpose, and this purpose alone, the Examiner introduced Feistel. Thus, as indicated below, no combination of Carter and Feistel teaches or suggests claim 3.

i. No combination of Carter and Feistel teach or suggests Appellant's acquiring matched keys for each group

Claim 3 provides, *inter alia*, that a public key and a matched private key is acquired for each group. The Examiner appears to suggest that Carter discloses group keys on page 9, as follows:

> . . . encrypting the document key with the public key of the collaborative group (see column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100). . .

The passage cited by the Examiner is reproduced as follows:

> The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question., which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key.

It is clear from this passage that each member, and not each group, has a public key and a corresponding private key. Further, Figure 5 indicates that an encrypted document key, whatever that may be, is part of the member definition, not any sort of group.

Feistel does not appear to address acquiring matched keys for each group.

ii. No combination of Carter and Feistel teach or suggests Appellant's formula for gaining access

Claim 3 provides, *inter alia*, for an access formula expressing logical combination of the at least one group for which access to an information set will be granted. Carter does not teach a *formula* for gaining access.

The Examiner's support that Carter discloses Applicant's access formula is provided on page 4 as follows:

> Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 13, lines 18-38). The Carter method would be inoperative if such a comparison were not made.

The passage cited by the Examiner is reproduced as follows (emphasis added):

> During an identifying step 114, a collaborative group is identified by identifying one or more members of the group. Identification is accomplished by obtaining user identifiers 48 through dialog boxes or other interactive user interfaces, by identifying a group object 70 or other group identifier that is known to the operating system 46, or by other identification means familiar to those of skill in the art. In one embodiment, a default mechanism is employed whereby the user presently directing the collaborative access controller 44 is automatically identified as a member of the collaborative group.
> During a member-key-obtaining step 116, the collaborative access controller 44 obtains one public key 78 for each collaborative group member. In some embodiments, the step 116 includes accessing the database system 62. In one of these embodiments, the collaborative access controller 44 submits one or more requests for public keys 78 to the authenticator 64, and the public keys 78 are supplied only after the requests are validated. Validation uses familiar techniques to verify that the source of the access request has sufficient access rights.

This passage clearly neither teaches nor suggests a formula of any kind, let alone Appellant's access formula. In fact, if anything, this section discloses keys assigned to individual members thereby granting direct access to each member.

Feistel does not appear to address access formulas.

Claim 3 is patentable over any combination of Carter and Feistel. Claims 4 and 5 depends from claim 3 and are therefore also patentable.

E. Whether claim 7 is unpatentable under 35 U.S.C. § 103(a) over Carter in view of Feistel

Claim 7, which depends from claim 3, provides a method for the secure handling of information wherein *the access formula is a boolean combination of groups*. A group asserts true in the boolean combination when a consumer client member of the group requests access to the information set protected by the access formula. The consumer client group member is granted access if the access formula resultant is true.

The Examiner rejected claim 7 with the following argument at page 10:

> As per claim 7, Carter points out that the member is verified if the corresponding identifier is found . . . Carter does not explicitly disclose the feature of a boolean combination resultant of true [*sic*]. However, this feature is deemed to be inherent to the method of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The method of Carter would be inoperative if this logical consequence did not result.

This is substantially the same argument used by the Examiner in rejecting claim 11 as anticipated by Carter, which was argued in Section C above. The combination of Carter with Feistel adds nothing new to the Examiner's argument.

Claim 7 is patentable over any combination of Carter and Feistel. Carter and Feistel neither teach nor suggest an access formula that is a boolean combination of groups. Thus, even if claim 3 is deemed unpatentable, claim 7 is still patentable.

A fee of $320 as applicable under the provisions of 37 C.F.R. § 1.17(c). Please charge this fee and charge any additional fee or credit any overpayment in connection with this filing to Deposit Account No. 19-4545. A duplicate of this notice is enclosed for this purpose.

Respectfully submitted,

JAMES P. HUGHES

By: _____
Mark D. Chuey, Ph.D.
Registration No. 42,415
Agent for Applicant

Date: January 31, 2003

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendix

IX. APPENDIX - CLAIMS ON APPEAL

1. A method for the secure handling of information encrypted to a data set, the information requested by a requesting consumer client, the data set stored on at least one storage device, the method comprising decrypting a value required to decrypt the information, the value decrypted by correctly solving an access formula describing a function of groups, each group comprising a list of at least one client, wherein the requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula.

2. A method for the secure handling of information as in claim 1 wherein the encrypted value and the access formula are stored as metadata in the data set.

3. A method for the secure handling of information by at least one client using at least one untrusted storage device, each client connected to the at least one untrusted storage device using a network, the network further having a key manager for issuing private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key, the method comprising:

creating at least one group, each group comprising a list of at least one consumer client;

acquiring a public key and a matched private key for each of the at least one group;

encrypting an information set to produce a data set, the encryption based on a randomly generated number;

determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a consumer client belonging to the at least one solution group may access the encrypted information set;

asymmetrically encrypting the randomly generated number using the determined access formula and the public key for each of the at least one group granted access to the information set;

adding the encrypted randomly generated number to the data set; and

storing the data set on at least one untrusted storage device.

4. A method for the secure handling of information as in claim 3 wherein a consumer client having a public key and a matched private key requests access to information encrypted in the stored data set, the method further comprising:

receiving a request from the consumer client;

determining if the consumer client belongs to at least one solution group which solves the access formula and, if not, denying access;

otherwise, decrypting the randomly generated number using the private key for the at least one determined solution group; and

encrypting the randomly generated number using the public key for the consumer client thereby permitting access to the encrypted information set by the consumer client.

5. A method for the secure handling of information as in claim 4 further comprising recording all attempts to access the information set in an audit trail, the audit trail including an indication of the consumer client requesting access.

6. A method for the secure handling of information as in claim 3 wherein a plurality of groups form a solution to the access formula, asymmetrically encrypting the randomly generated number creating an encrypted partial key for each group in the plurality of groups, each partial key encrypted using the public key for one group in the plurality of groups, each partial key required to decrypt the encrypted randomly generated number, the method further comprising:

for each group in the plurality of groups, decrypting the encrypted partial key using the private key for the group;

for each group in the plurality of groups, reencrypting the decrypted partial key using the public key for a requesting client;

decrypting each reencrypted partial key using the private key of the requesting client;

determining the randomly generated number based on each partial key; and

decrypting the information set using the determined randomly generated number.

7. A method for the secure handling of information as in claim 3 wherein the access formula is a boolean combination of groups, a group asserting true in the boolean combination when a consumer client member of the group requests access to the information set protected by the access formula, the consumer client group member granted access if the access formula resultant is true.

8. A method for the secure handling of information as in claim 3 further comprising:

determining that an information set destined for storage on at least one untrusted storage device is encrypted; and

prohibiting storage on the at least one untrusted storage device if the information set is determined not to be encrypted.

9. A system for the secure handling of information stored on at least one untrusted storage device connected to a network comprising:

a key manager connected to the network, the key manager operable to generate private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key;

at least one group server connected to the network, each group server operable to

(a) maintain at least one group, each group comprising a list of client members allowed access to information produced by any client member of the group, and

(b) obtain a private key and matched public key for each group; and

at least one producer client connected to the network, the producer client operative to

(a) encrypt an information set to produce a data set, the encryption based on an encryption value,

(b) determine an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the

access formula by at least one solution group indicating that a client belonging to the at least one solution group may access the encrypted information set,

(c) asymmetrically encrypt the encryption value using the determined access formula and the public key for each of the at least one group for which access to the information set may be granted,

(d) add the encrypted encryption value and the access formula to the data set, and

(e) store the data set on at least one untrusted storage device.

10. A system for the secure handling of information as in claim 9 wherein the encryption value comprises a randomly generated number.

11. A system for the secure handling of information as in claim 9 wherein the access formula is a boolean combination of groups, a group asserting true in the boolean combination when a client member of the group requests access to the information set protected by the access formula, the client member granted access if the access formula resultant is true.

12. A system for the secure handling of information as in claim 9 wherein the producer client is further operable to

determine that an information set destined for storage on at least one untrusted storage device is encrypted; and

prohibit storage on to the at least one untrusted storage device if the information set is determined not to be encrypted.

13. A system for the secure handling of information as in claim 9 further comprising at least one consumer client connected to the network, each consumer client operative to

obtain a private key and a matched public key;

determine that an accessed data set has encrypted information;

determine at least one group server maintaining at least one group from the access formula logical combination, the at least one group forming a solution to the access formula;

send a request to access the encrypted information set to each of the at least one determined group server;

if access is granted from each of the determined at least one group server, decrypt the encryption value using the obtained private key; and

decrypt the encrypted information set using the decrypted encryption value.

14. A system for the secure handling of information as in claim 13 wherein the at least one group is a plurality of groups and wherein the producer client asymmetrically encrypts the encryption value to produce a partial key for each group in each set of groups forming a solution to the access formula, the consumer client further operative to decrypt the encryption value by decrypting each partial key and to determine the encryption value based on each decrypted partial key.

15. A system for the secure handling of information as in claim 13 wherein each group server is further operable to

receive a request from a requesting consumer client;

determine if the requesting consumer client belongs to at least one solution group which solves the access formula and, if not, deny access;

otherwise, decrypt the encryption value using the private key for the at least one determined solution group; and

encrypt the encryption value using the public key for the requesting consumer client thereby permitting access to the encrypted information set by the consumer client.

16. A system for the secure handling of information as in claim 13 wherein each group server is further operable to record all attempts to access each

information set in an audit trail, the audit trail including an indication of the consumer client requesting access.

17. A system for the secure handling of information as in claim 13 wherein each group server is further operable to permit additions, deletions, and changes to each group list of client members.